International Journal of Competitive Intelligence, Strategic, Scientific and Technology Watch
SciWatch Journal 1 (2008), Issue 1, 92 - 93

REVIEW OF ARTICLE: "Benchmarking R&D and companies through patent analysis using free databases and special software: a tool to improve innovative thinking".

Henri Jean-Marie Dou (2004)

(Review by M. Welling Flensborg)
e-mail: m.welling.flensborg@gmail.com

It is a fact that the latest trends in the business world call for benchmarking activities, thus defining a system to compare the activities of the company with those of the best performers in this field.

In other words, in a world increasingly marked by strong competition, all organizations, in order to survive, need to get information from competitors, so that they can learn and improve by observing their direct competitors.

Either way, there should be a limit to divide benchmarking from industrial espionage, concept that even though we think is more related with fiction novels, it is quite often a reality, and it is indeed a non conventional way of doing intelligence gathering.

Even when it is a fact that representatives of the industrial world, such as the Society of Competitive Intelligence Professionals (SCIP), recognize that the competitive intelligence is not only ethical but also necessary to survive in the market, it is equally clear that there has to be a red line that cannot be surpassed in the benchmarking activities, all in order to avoid industrial espionage. This practice is universally considered to be against the principals not only of ethics, but also of the law, and it is therefore unacceptable.

But how can we define what is illegal in a field where the rapid advance of technology is clearly incompatible with the times of the law? When is it that practices that were once acceptable become illegal?

Andrew Crane suggests three criteria to guide us with the ethical issues that may arise during intelligence gathering operations. In his opinion we have to evaluate the problem from several points of view: Firstly we have to consider the way information is provided (using tactics that can be more or less ethical or legal), then we should consider the object of that research (the information could be private or confidential) and finally we must consider the final goal of that research (that or those goals could be against public interest).

But when does the gathering of information become questionable? The possibilities are many: from the clearly illegal practices to the practices that are “only” against common deontological principles, or against the “golden rules”, including anything that might violate the obligations of loyalty and honesty in business matters. Besides, determining when information has to be considered confidential or private is not as easy as it might seem, because most modern corporations have structures without defined limits, and because of their tendency to deal with increasingly more

people for its activities, which, moreover, are often carried out in public or semi-public environments that are easily observable.

In fact, although the significant investments made by corporations share the imperative need to protect intellectual property, the rapid development of communication and information technologies makes it increasingly easy to access and use data protected by intellectual property rights, making the issue of hacking or theft of sensitive digital information, a crucial problem, in front of which justice is not ready, especially because most of these operations take place in a transnational space nearly impossible to monitor.

But new technology is not the only factor threatening intellectual property: national cultures can also be a threat to this kind of legal protection: for example, we should not forget that in Asian cultures it is very common to share information for the sake of general progress of the society.

The concept of public interest concerns mainly the anti-competitive behaviors, but the growing collaboration between private and government public agencies for the development of products and services related with national security issues, creates situations in which access to confidential or sensitive data might in some cases involve threats to public interest. We should also consider that in certain sectors, such as the medical sector, commercial confidentiality can actually act against the public interest.

In conclusion, it is a fact that with the increasing development of knowledge-based environments, incentives and opportunities for surpassing the limits in intelligence gathering activities have increased exponentially. It is also certain that the growing number of partnerships and common goals shared between the activities of states and private companies create the need, in the business world, to protect the integrity and security of data and privacy policies. Therefore, the establishment of strong confidence relationships between the main stakeholders involved becomes a key factor when it comes to performing a legal and ethic intelligence gathering activity.